AMENDMENTS TO THE CLAIMS

1. (CURRENTLY AMENDED) A computer-implemented method for executing an untrusted program, comprising:

establishing a limited environment within a general environment, wherein said limited environment comprises ~~at least~~ one or more mock resources ~~resource~~, wherein said general environment comprises ~~at least~~ one or more real resources ~~resource~~, ~~and~~ wherein said limited environment and said general environment are both ~~implemented using~~ provided by the same ~~type of~~ operating system, and wherein programs executing within said limited environment cannot access the one or more real resources in said general environment;

executing at least a portion of an untrusted program within said limited environment; and

examining said limited environment after execution of at least said portion of said untrusted program to check for undesirable behavior exhibited by said untrusted program.

2. (CANCELLED).

3. (ORIGINAL) The method of claim 1, wherein said limited environment comprises a shell in a UNIX operating system environment.

4. (CURRENTLY AMENDED) The method of claim 1, wherein examining said limited ~~mock~~ environment comprises:

determining whether ~~said~~ a particular mock resource of said one or more mock resources has been deleted.

5. (CURRENTLY AMENDED) The method of claim 1, wherein examining said limited ~~mock~~ environment comprises:

determining whether ~~said~~ a particular mock resource of said one or more mock resources has been renamed.

6. (CURRENTLY AMENDED) The method of claim 1, wherein examining said limited ~~mock~~ environment comprises:

determining whether ~~said~~ a particular mock resource of said one or more mock resources has been moved.

7. (CURRENTLY AMENDED) The method of claim 1, wherein examining said limited ~~mock~~ environment comprises:

determining whether ~~said~~ a particular mock resource of said one or more mock resources has been altered.

8. (CURRENTLY AMENDED) The method of claim 7, wherein said particular mock resource has a parameter associated therewith which changes when said particular mock resource is altered, and wherein determining whether said particular mock resource has been altered, comprises:

determining whether said parameter has changed.

9. (CURRENTLY AMENDED) The method of claim 8, wherein said parameter is a time value indicating when said particular mock resource was last updated.

10. (CURRENTLY AMENDED) The method of claim 1, wherein examining said limited ~~mock~~ environment comprises:

determining whether said particular mock resource has been accessed.

11. (CURRENTLY AMENDED) The method of claim 10, wherein said particular mock resource contains one or more sets of content, wherein said untrusted program executes in a particular portion of memory, and wherein determining whether said particular mock resource has been accessed comprises:

searching said particular portion of said memory for at least one of said one or more sets of content.

12. (ORIGINAL) The method of claim 1, further comprising:

providing information indicating behavior exhibited by said untrusted program.

13. (ORIGINAL) The method of claim 12, wherein said information comprises indications of undesirable behavior exhibited by said untrusted program.

14. (ORIGINAL) The method of claim 1, further comprising:

determining whether said untrusted program has exhibited undesirable behavior; and

in response to a determination that said untrusted program has exhibited undesirable behavior, taking corrective action.

15. (ORIGINAL) The method of claim 14, wherein taking corrective action comprises:

deleting said untrusted program.

16. (ORIGINAL) The method of claim 14, wherein taking corrective action comprises: providing a warning to a user.

17. (CURRENTLY AMENDED) A computer readable medium comprising instructions which, when executed by one or more processors, cause the one or more processors to execute an untrusted program, said computer readable medium comprising:

establishing a limited environment within a general environment, wherein said limited environment comprises ~~at least~~ one or more mock resources ~~resource~~, wherein said general environment comprises ~~at least~~ one or more real resources ~~resource~~, ~~and~~ wherein said limited environment and said general environment are both ~~implemented using~~ provided by the same ~~type of~~ operating system, and wherein programs executing within said limited environment cannot access the one or more real resources in said general environment;

executing at least a portion of an untrusted program within said limited environment; and

examining said limited environment after execution of at least said portion of said untrusted program to check for undesirable behavior exhibited by said untrusted program.

18. (CANCELLED).

19. (ORIGINAL) The computer readable medium of claim 17, wherein said limited environment comprises a shell in a UNIX operating system environment.

20. (CURRENTLY AMENDED) The computer readable medium of claim 17, wherein said instructions for causing one or more processors to examine said limited ~~mock~~ environment comprises:

instructions for causing one or more processors to determine whether ~~said~~ a particular mock resource of said one or more mock resources has been deleted.

21. (CURRENTLY AMENDED) The computer readable medium of claim 17, wherein said instructions for causing one or more processors to examine said limited ~~mock~~ environment comprises:

instructions for causing one or more processors to determine whether ~~said~~ a particular mock resource of said one or more mock resources has been renamed.

22. (CURRENTLY AMENDED) The computer readable medium of claim 17, wherein said instructions for causing one or more processors to examine said limited ~~mock~~ environment comprises:

instructions for causing one or more processors to determine whether ~~said~~ a particular mock resource of said one or more mock resources has been moved.

23. (CURRENTLY AMENDED) The computer readable medium of claim 17, wherein said instructions for causing one or more processors to examine said limited ~~mock~~ environment comprises:

instructions for causing one or more processors to determine whether ~~said~~ a particular mock resource of said one or more mock resources has been altered.

24. (CURRENTLY AMENDED) The computer readable medium of claim 23, wherein said particular mock resource has a parameter associated therewith which changes when said particular mock resource is altered, and wherein said instructions for causing one or more processors to determine whether said particular mock resource has been altered, comprises:

instructions for causing one or more processors to determine whether said parameter has changed.

25. (CURRENTLY AMENDED) The computer readable medium of claim 24, wherein said parameter is a time value indicating when said particular mock resource was last updated.

26. (CURRENTLY AMENDED) The computer readable medium of claim 17, wherein said instructions for causing one or more processors to examine said limited ~~mock~~ environment comprises:

instructions for causing one or more processors to determine whether said particular mock resource has been accessed.

27. (CURRENTLY AMENDED) The computer readable medium of claim 26, wherein said particular mock resource contains one or more sets of content, wherein said untrusted program executes in a particular portion of memory, and wherein said instructions for causing one or more processors to determine whether said particular mock resource has been accessed comprises:

instructions for causing one or more processors to search said particular portion of said memory for at least one of said one or more sets of content.

28. (ORIGINAL) The computer readable medium of claim 17, further comprising:

instructions for causing one or more processors to provide information indicating behavior exhibited by said untrusted program.

29. (ORIGINAL) The computer readable medium of claim 28, wherein said information comprises indications of undesirable behavior exhibited by said untrusted program.

30. (ORIGINAL) The computer readable medium of claim 17, further comprising:

instructions for causing one or more processors to determine whether said untrusted program has exhibited undesirable behavior; and

instructions for causing one or more processors to, in response to a determination that said untrusted program has exhibited undesirable behavior, take corrective action.

31. (ORIGINAL) The computer readable medium of claim 30, wherein said instructions for causing one or more processors to take corrective action comprises:

instructions for causing one or more processors to delete said untrusted program.

32. (ORIGINAL) The computer readable medium of claim 30, wherein said instructions for causing one or more processors to take corrective action comprises:

instructions for causing one or more processors to provide a warning to a user.

33. (CANCELLED).

34. (CANCELLED).

35. (CANCELLED).

36. (CANCELLED).